

George Haines, Esq.
Nevada Bar No. 9411
Gerardo Avalos, Esq.
Nevada Bar No. 15171
FREEDOM LAW FIRM
8985 S. Eastern Ave., Suite 350
Las Vegas, NV 89123
Tele. 702.880.5554
E-fax: 702.967.6666
Email: info@freedomlegalteam.com

Michael Kind, Esq.
Nevada Bar No. 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Phone: (702) 337-2322
FAX: (702) 329-5881
Email: mk@kindlaw.com

Attorneys for Plaintiff Jehu Bryant and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

Jehu Bryant, individually and on behalf of
all others similarly situated,

Plaintiff,

-vs.-

MX Holdings US, Inc. CFP Fire Protection,
Inc., COSCO Fire Protection, Inc., and
Firetrol Protection Systems, Inc.

Defendants.

CASE NO.

CLASS ACTION

**Complaint for Damages Based on: (1)
Negligence; (2) Invasion of Privacy; (3)
Breach of Contract; and (4) Breach of
Implied Contract**

Jury Trial Demanded

Exempt from Arbitration

Introduction

1. Defendants MX Holdings US, Inc. CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc., (“Defendants”) failed to safeguard the confidential personal identifying information of Plaintiff Jehu Bryant (“Plaintiff”) and thousands of individuals (“Class Members” or collectively as the “Class”). This class action is brought on behalf of Class Members whose personally identifiable information (“PII” or “Private Information”) was stolen by cybercriminals in a cyber-attack that accessed sensitive patient information through Defendants’ email accounts.
2. On or about October 28, 2021, Defendants became aware that a group of cybercriminals had access to Defendants’ email accounts.
3. On or about April 5, 2022, more than five months later, Defendants determined that the information accessed by the cybercriminals contained personal information belonging to the Class Members.
4. Plaintiff and Class Members were not notified of the data breach until May, 2022, more than six months after their information was first accessed.
5. The cybercriminals accessed insufficiently protected information belonging to Plaintiff and the Class Members. Upon information and belief, as a result of Defendants’ failure to properly secure Plaintiff’s and the Class Members’ personal information, the cybercriminals obtained extensive personal information including names, dates of birth, social security numbers, driver’s license numbers, passport numbers, financial account numbers, and medical information, collectively known as personally identifiable information (“PII” or “Private Information”).
6. Plaintiffs’ and Class Members’ sensitive personal information, which was entrusted to Defendants, their officials and agents, was compromised, unlawfully accessed, and stolen due to the Data breach.
7. As a result of Defendants’ actions and/or inaction, Plaintiff and the Class Members were harmed and must now take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all of the Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to

1 unauthorized credit card charges, unauthorized access to email accounts, identity theft, and
2 other fraudulent use of their financial accounts.

3 8. Defendants' wrongful actions and/or inaction constitute common law negligence, invasion
4 of privacy by the public disclosure of private facts, breach of contract, and breach of implied
5 contract.

6 9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address
7 Defendants' inadequate safeguarding of Class Members' Private Information that they
8 collected and maintained, and for failing to provide timely and adequate notice to Plaintiff
9 and other Class Members that their information had been subject to the unauthorized access
10 of an unknown third party.

11 10. Plaintiff, on behalf of himself and the Class seeks (i) actual damages, economic damages,
12 emotional distress damages, statutory damages and/or nominal damages, (ii) exemplary
13 damages, (iii) injunctive relief, and (iv) fees and costs of litigation.

14 **Jurisdiction and Venue**

15 11. This Court has subject matter jurisdiction over this action under the Class Action Fairness
16 Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated
17 claims of the individual Class Members exceed the sum or value of \$5,000,000
18 exclusive of interest and costs, and, upon information and belief, members of the
19 proposed Class are citizens of states different from Defendants.

20 12. This Court has jurisdiction over Defendants through their business operations in this
21 District, the specific nature of which occurs in this District. Defendants intentionally avail
22 himself of the markets within this District to render the exercise of jurisdiction by this Court
23 just and proper.

24 13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part
25 of the events and omissions giving rise to this action occurred in this District, and because
26 Plaintiff resides in this District.

27 **Parties**

28 14. Plaintiff is a natural person residing in Clark County, Nevada.

29 15. Defendants are corporations that provide building construction, safety, and fire protection
services. Defendants operate nationally, including in Nevada.

Factual Allegations

16. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.
17. According to the Federal Trade Commission ("FTC"):
- Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.
18. The United States Government Accountability Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO explained that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."
19. Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.
20. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.
21. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed by Defendants.

22. The FTC has issued a publication entitled “Protecting Personal Information: A Guide for Business” (“FTC Report”). The FTC Report provides guidelines for businesses on how to develop a “sound data security plan” to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:
- a. Know what personal information you have in your files and on your computers;
 - b. Keep only what you need for your business;
 - c. Protect the information that you keep;
 - d. Properly dispose of what you no longer need;
 - e. Control access to sensitive information by requiring that employees use “strong” passwords; tech security experts believe the longer the password, the better; and
 - f. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.
23. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.
24. The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
25. Upon information and belief, Defendants have policies and procedures in place regarding the safeguarding of confidential information they are entrusted with and Defendants failed to comply with those policies. Defendants also negligently failed to comply with industry standards or even implement rudimentary security practices, resulting in Plaintiff’s and the Class’ confidential information being substantially less safe than had this information been entrusted with other similar companies.
26. On or around May 10, 2022, Plaintiff and thousands of Class Members received letters from Defendants notifying them that Defendants learned of suspicious activity that allowed one or more cybercriminals to access their systems containing Plaintiff’s and the Class’ Personally Identifiable Information.

- 1 27. The criminals were able to access Plaintiff's and the Class' personal information because
2 Defendants failed to take reasonable measures to protect the Personally Identifiable
3 Information they collected and stored. Among other things, Defendants failed to implement
4 data security measures designed to prevent this attack, despite repeated industry wide
5 warnings about the risk of cyberattacks and the highly publicized occurrence of many
6 similar attacks in the recent past.
- 7 28. Defendants' notice of Data breach was not just untimely but woefully deficient, failing to
8 provide basic details, including but not limited to, how unauthorized parties accessed their
9 accounts, whether the information was encrypted or otherwise protected, how they learned
10 of the Data breach, whether the breach occurred system-wide, whether servers storing
11 information were accessed, and how many individuals were affected by the Data breach.
- 12 29. As a result of Defendants' failure to properly secure Plaintiff's and the Class Members'
13 personal identifying information, Plaintiff's and the Class Members' privacy has been
14 invaded.
- 15 30. Moreover, all of this personal information is likely for sale to criminals on the dark web,
16 meaning that unauthorized parties have accessed and viewed Plaintiff's and the Class
17 Members' unencrypted, non-redacted information, including names, dates of birth, social
18 security numbers, driver's license numbers, passport numbers, financial account numbers,
19 and medical information, and more.
- 20 31. Armed with the Private Information accessed in the cyber-attack, data thieves can commit
21 a variety of crimes including, e.g., opening new financial accounts in Class Members'
22 names, taking out loans in Class Members' names, using Class Members' names to obtain
23 medical services, using Class Members' health information to target other phishing and
24 hacking intrusions based on their individual health needs, using Class Members'
25 information to obtain government benefits, filing fraudulent tax returns using Class
26 Members' information, obtaining driver's licenses in Class Members' names but with
27 another person's photograph, and giving false information to police during an arrest.
- 28 32. Given all of the information obtained, the criminals would also be able to create numerous
29 fake accounts and sell sensitive health information, as part of their identity theft operation.

33. As a direct and proximate result of Defendants' wrongful disclosure, criminals now have Plaintiff's and the Class Members' personal identifying information. Additionally, the disclosure makes Plaintiff and Class Members much more likely to respond to requests from Defendants or law enforcement agencies for more personal information, such as bank account numbers, login information or even Social Security numbers. Because criminals know this and are capable of posing as Defendants or law enforcement agencies, consumers like Plaintiff and fellow Class Members are more likely to unknowingly give away their sensitive personal information to other criminals.

34. Defendants' wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendants' wrongful actions and/or inaction, Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

35. As a further result of the data breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

36. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the Data breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

37. As a direct and proximate result of the data breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam

1 messages and e-mails received as a result of the data breach. Plaintiffs and Class Members
2 have likewise suffered and will continue to suffer an invasion of their property interest in
3 their own Private Information such that they are entitled to damages for unauthorized access
4 to and misuse of their Private Information from Defendant. Plaintiffs and Class Members
5 presently and will continue to suffer from damages associated with the unauthorized use
6 and misuse of their Private Information as thieves will continue to use the stolen information
7 to obtain money and credit in their name for several years.

8 38. Defendants were at all times fully aware of their obligations to protect the Private
9 Information of Plaintiff and Class Members. Plaintiff and Class Members would not have
10 entrusted their Private Information to Defendants had they known that Defendants would
11 fail to maintain adequate data security. Defendants were also aware of the significant
12 repercussions that would result from their failure to do so.

13 39. Accordingly, Plaintiff on behalf of himself and the Class, brings this action against
14 Defendants seeking redress for their unlawful conduct.

15 **Class Action Allegations**

16 40. Pursuant to Federal Rule of Civil Procedure 23 Plaintiff bring this class action on behalf of
17 himself and the following Class of similarly situated individuals:

18 All persons whose sensitive personal information, including, but not
19 limited to, names, dates of birth, social security numbers, driver's
20 license numbers, passport numbers, financial account numbers, and
21 medical information was obtained by an unauthorized individual or
individuals from Defendants during the October 2021 data breach.

22 41. The Class specifically excludes Defendants and their officers, directors, and/or agents, the
23 Court, and Court personnel.

24 42. The putative Class is comprised of thousands of persons, making joinder impracticable. The
25 joinder of the Class Members is impractical and the disposition of their claims in the Class
26 action will provide substantial benefits both to the parties and to the Court. The Class can
27 be identified through Defendants' records or Defendants' agents' records.

28 43. The rights of each Class Member were violated in an identical manner as a result of
29 Defendants' willful, reckless and/or negligent actions and/or inaction.

- 1 44. The questions of law and fact common to all Class Members, and which predominate over
2 any questions affecting only individual Class Members, are as follows:
- 3 a. Whether Defendants negligently failed to maintain and execute reasonable procedures
4 designed to prevent unauthorized access to Plaintiff's and Class Members' personal
5 identifying information;
- 6 b. Whether Defendants were negligent in storing and failing to adequately safeguard
7 Plaintiff's and Class Members' personal identifying information;
- 8 c. Whether Defendants owed a duty to Plaintiff and Class Members to exercise reasonable
9 care in protecting and securing their personal identifying information;
- 10 d. Whether Defendants breached their duties to exercise reasonable care in failing to protect
11 and secure Plaintiff's and Class Members' personal identifying information;
- 12 e. Whether by disclosing Plaintiff's and Class Members' personal identifying information
13 without authorization, Defendants invaded Plaintiff's and Class Members' privacy;
- 14 f. Whether Defendants created an implied contract with Plaintiff and Class Members to keep
15 their personal identifying information confidential; and
- 16 g. Whether Plaintiff and Class Members sustained damages as a result of Defendants' failure
17 to secure and protect their personal identifying information.
- 18 45. Plaintiff and his counsel will fairly and adequately represent the interests of Class Members.
19 Plaintiff has no interests antagonistic to, or in conflict with, Class Members' interests.
20 Plaintiff's attorneys are highly experienced in the prosecution of consumer class action,
21 complex litigation and privacy breach cases.
- 22 46. Plaintiff's claims are typical of Class Members' claims in that Plaintiff's claims and Class
23 Members' claims all arise from Defendants' wrongful disclosure of their personal
24 identifying information and from Defendants' failure to properly secure and protect the
25 same.
- 26 47. A class action is superior to other available methods for the fair and efficient adjudication
27 of the controversy. Class treatment of common questions of law and fact is superior to
28 multiple individual actions or piecemeal litigation. Absent a class action, most class
29 members would likely find that the cost of litigating their individual claim is prohibitively

high and would therefore have no effective remedy. Defendants would retain the benefits of their wrongdoing despite its serious violations of the law.

48. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendants. In contrast, the adjudication of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

49. Defendants have acted or failed to act on grounds that apply generally to the class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

50. Class certification, therefore, is appropriate pursuant to Rule 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

**First Cause of Action
Negligence**

51. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

52. Upon Defendants' accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

53. Defendants owed a duty of care not to subject Plaintiff's and the Class' Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

54. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' personal identifying information would result in an unauthorized third party gaining access to such information

1 for no lawful purpose, and that such third parties would use Plaintiff's and Class Members'
2 personal identifying information for malevolent and unlawful purposes, including the
3 commission of direct theft and identity theft.

4 55. Defendants knew, or should have known, of the risks inherent in collecting, storing, and
5 sharing Private Information amongst themselves and the importance of adequate security.
6 Defendants knew of should have known about numerous well-publicized data breaches
7 within the industry.

8 56. Plaintiff and the Class Members were (and continue to be) damaged as a direct and
9 proximate result of Defendants' failure to secure and protect their personal identifying
10 information as a result of, *inter alia*, direct theft, identity theft, expenses for credit
11 monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket
12 expenses, anxiety, emotional distress, loss of privacy, and other economic and non-
13 economic harm, for which they suffered loss and are entitled to compensation.

14 57. Defendants' wrongful actions and/or inaction (as described above) constituted (and
15 continue to constitute) negligence at common law.

16 **Second Cause of Action**
17 **Invasion of Privacy by Public**
18 **Disclosure of Private Facts and Intrusion Upon Seclusion**

19 58. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

20 59. Plaintiff's and Class Members' personal identifying information is and always has been
21 private information.

22 60. Dissemination of Plaintiff's and Class Members' private information is not of a legitimate
23 public concern; publication to third parties of their personal identifying information would
24 be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable
25 people.

26 61. Plaintiff and the Class Members were (and continue to be) damaged as a direct and
27 proximate result of Defendants' invasion of their privacy by publicly disclosing their private
28 facts including, *inter alia*, direct theft, identity theft, expenses for credit monitoring and
29 identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy,
and other economic and non-economic harm, for which they are entitled to compensation.

62. Defendants' wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their personal identifying information).

Third Cause of Action
Breach of Contract

63. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

64. Plaintiff and other Class Members entered into valid and enforceable express contracts with Defendants under which Plaintiff and other Class Members agreed to provide their Private Information to Defendants, and Defendants impliedly, if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

65. To the extent Defendants' obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendants to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with FCC regulations; federal, state and local laws; and industry standards. Neither Plaintiff nor any Class member would have entered into these contracts with Defendants without the understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

66. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for Defendants' agreement to protect the confidentiality of that Private Information.

67. The protection of Plaintiff's and Class Members' Private Information was a material aspect of Plaintiff's and Class Members' contracts with Defendants.

68. Defendants' promises and representations described above relating to FCC regulations and industry practices, and Defendants' purported concern about its clients' privacy rights became terms of Plaintiff's and Class Members' contracts with Defendants. Defendants

1 breached these promises by failing to comply with FCC regulations and reasonable industry
2 practices.

3 69. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided
4 by Defendants and/or otherwise understood that Defendants would protect their Private
5 Information if that information was provided to Defendants.

6 70. Plaintiff and Class Members fully performed their obligations under the implied contract
7 with Defendants; however, Defendants did not.

8 71. As a result of Defendants' breach of these terms, Plaintiff and Class Members have suffered
9 a variety of damages including but not limited to: the lost value of their privacy; not getting
10 the benefit of their bargain with Defendants; the lost difference in the value between the
11 secure services Defendants promised and the insecure services received; the value of the lost
12 time and effort required to mitigate the actual and potential impact of the data breach on their
13 lives, including, inter alia, the requirement to place "freezes" and "alerts" with credit reporting
14 agencies, to contact financial institutions, to close or modify financial and medical accounts,
15 to closely review and monitor credit reports and various accounts for unauthorized activity,
16 and to file police reports. Additionally, Plaintiff and Class Members have been put at an
17 increased risk of future identity theft, fraud, and/or misuse of their Private Information, which
18 may take years to manifest, discover, and detect.

19 72. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust
20 enrichment, disgorgement, declaratory and injunctive relief, and fees and costs of litigation.

21 **Fourth Cause of Action**
22 **Breach of Implied Contract**

23 73. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

24 74. "Where the terms of a contract are literally complied with but one party to the contract
25 deliberately contravenes the intention and spirit of the contract, that party can incur liability
26 for breach of the implied covenant of good faith and fair dealing." *Hilton Hotels Corp. v.*
27 *Butch Lewis Prods., Inc.*, 107 Nev. 226, 232 (1991).

28 75. Among other things, Plaintiff and Class Members were required to disclose their personal
29 identifying information to Defendants for the provision of employment and services, as well

as implied contracts for the Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

76. When Plaintiff and Class Members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

77. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

78. Under implied contracts, Defendants and/or their affiliated providers promised and were obligated to protect Plaintiff's and Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information.

79. The implied contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information, are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' Data breach notification letters and Defendants' notices of privacy practices.

80. Defendants' express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

81. Plaintiff and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendants' employment services.

82. Defendants materially breached their contractual obligations to protect the private information Defendants gathered when the information was accessed and exfiltrated during the data breach.

83. Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy practices. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by their notification of the data breach to Plaintiff and Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section

5 of the FTCA, or otherwise protect Plaintiff's and Class Members' private information as set forth above.

84. The data breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

85. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain they entered into, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the secure services Defendants promised and the insecure services received.

86. Had Defendants disclosed that their security was inadequate or that they did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have entered into the aforementioned contracts with Defendants.

87. As a direct and proximate result of the data breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

Prayer for Relief

88. Wherefore, Plaintiff, individually and on behalf of the other members of the Class proposed in this complaint, respectfully requests that the Court enter judgement in favor of Plaintiff and the Class against Defendants, as follows:

- Certifying this action as a class action, with a class as defined above;
- For equitable relief enjoining Defendants from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- Awarding compensatory damages to redress the harm caused to Plaintiff

1 and Class Members in the form of, *inter alia*, direct theft, identity theft,
2 expenses for credit monitoring and identity theft insurance, out-of-
3 pocket expenses, anxiety, emotional distress, loss of privacy, and other
4 economic and non-economic harm. Plaintiff and Class Members also are
5 entitled to recover statutory damages and/or nominal damages.
6 Plaintiff's and Class Members' damages were foreseeable by Defendants
7 and exceed the minimum jurisdictional limits of this Court.

- 8 • Ordering injunctive relief including, without limitation, (i) adequate
9 credit monitoring, (ii) adequate identity theft insurance, (iii) instituting
10 security protocols in compliance with the appropriate standards and (iv)
11 requiring Defendants to submit to periodic compliance audits by a third
12 party regarding the security of personal identifying information in its
13 possession, custody and control.
- 14 • Awarding Plaintiff and the Class Members interest, costs and attorneys'
15 fees; and
- 16 • Awarding Plaintiff and the Class such other and further relief as this
17 Court deems just and proper.

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

29 ///

///

Trial by Jury

89. Pursuant to the seventh amendment to the Constitution of the United States of America and the Constitution of the State of Nevada, Plaintiff is entitled to, and demands, a trial by jury.

DATED this 27th day of May 2022.

Respectfully submitted,

FREEDOM LAW FIRM, LLC

/s/ Gerardo Avalos
George Haines, Esq.
Gerardo Avalos, Esq.
8985 South Eastern Ave., Suite 350
Las Vegas, NV 89123

Kind Law

/s/ Michael Kind
Michael Kind, Esq.
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123
*Attorneys for Plaintiff and on behalf
of all others similarly situated*